UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,971	04/06/2001	Olli Immonen	367.39437X00	8278

20457 7590 10/31/2005

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-3873

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/720,971	IMMONEN, OLLI	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14-40 and 42-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14-40 and 42-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 15 August 2005. Claims 1-3, 5, 14, 15, 19, 23-25, 46, 47, and 66-68 have been amended. No claims have been added or canceled. Claims 1-12, 14-40, and 42-68 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 15 August 2005 have been fully considered but they are not persuasive.

In reference to the rejection of Claim 14 under 35 U.S.C. 112, second paragraph, as being indefinite, Applicant argues the rejection is improper because the specification (at, for example, page 4) supports the practice of the invention as not limited to a smart card because a SIM card or other storage unit (indicated by "etc.") may be used. However, the Examiner notes that Applicant acknowledges that a SIM is a "type of smart card" (page 17, paragraph 0042 of the substitute specification filed with the present amendment). Thus, that the specification discloses that the separate unit is, for example, a smart card, a SIM card (i.e., a specific type of smart card), etc., does not definitely provide what other type of separate unit there may be aside from a smart card or subset thereof. A negative limitation is definite only if the boundaries of the patent protection sought are definite. Therefore, the negative limitation "without a smart card"

is indefinite because there is no written description of what else the separate unit could be. See MPEP § 2173.05(i).

In reference to the rejection of Claims 1, 3-12, 14-19, 21-24, 27-40, 42-44, and 46-68 under 35 U.S.C. 103(a) as unpatentable over Ichikawa, PCT Publication WO97/24831, in view of Anvret et al, European Publication EP 0538216, and specifically in reference to independent Claims 1, 5, 15, 19, 22, 23, 24, and 46, Applicant argues that neither Ichikawa nor Anvret provides for a master secret code as recited in the claims. Applicant further argues that Ichikawa discloses derived keys and not a master secret code that is stored. The Examiner respectfully disagrees with both of these assertions. Regarding the fact that Ichikawa discloses the derivation of keys, the Examiner believes that this does not preclude the storage of a master secret code or key; on the contrary, the Examiner notes that Applicant discloses that the master secrets of the present invention can be "used for key derivation" (page 14, paragraph 0032 of the substitute specification). Regarding Applicant's assertion that Ichikawa does not disclose storage of a master secret code as claimed, the Examiner believes that Ichikawa does disclose storage of the master key (see, for example, page 6, lines 16-18, where the master key is stored in a secure area of a smart card).

Regarding Applicant's request that the Examiner point out where the prior art suggests "utilization of storage of a secret code used to provide reconnection to avoid computation overhead of calculating keys each time a connection is made", the Examiner notes that Ichikawa does disclose storage of a secret code (page 6, lines 16-18, where the master key is stored) used for connections (see page 9, lines 13-23).

The fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985).

In reference to the rejection of Claims 2, 20, 25, 26, and 45 under 35 U.S.C. 103(a) as unpatentable over Ichikawa in view of Anvret, and further in view of Weiss, US Patent 5845519, Applicant argues that Weiss does not cure the deficiencies argued in reference to Ichikawa and Anvret. However, the Examiner has addressed these arguments, particularly regarding Ichikawa, above.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Specification

3. The disclosure is objected to because of the following informalities:

Applicant has not corrected all of the errors in the specification referred to in the previous Office action. The specification still appears to contain minor grammatical and typographical errors. Note that all page and paragraph references are to the substitute specification received 15 August 2005, and all line numbers refer to the line number within each paragraph. For example, on page 5, paragraph 0008, lines 3-5, the phrase "and may be re-used in another secure connection" does not appear to have a subject; on page 20, paragraph 0048, line 16, it appears that the reference to "encrypted

response 80" is intended to refer to "encrypted response 65"; and on page 22, pargraph 0054, line 4, it appears that "encryptation algorithm" is intended to read "encryption algorithm".

Appropriate correction is required. The above is not intended as an exhaustive list of errors, and Applicant's cooperation is requested in correcting any other errors of which Applicant may become aware in the specification.

Claim Objections

4. The objections to Claims 5 and 47 for informalities are withdrawn in light of the amendments to the claims.

5. Claim 24 is objected to because of the following informalities: Claim 24 recites the limitation "at least one a master secret code and at least one signature" in lines 17-18 of the claim. It appears that this is intended to read "at least one of a master secret code and at least one signature".

Appropriate correction is required.

6. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

The listing of claims includes two claims labeled as Claim 29. The first Claim 29 is identical to Claim 28, and has been disregarded; only the second Claim 29 has been considered. Applicant is required to delete the first Claim 29 from the listing of claims. The listing of claims further includes two claims labeled as Claim 46. The first Claim 46 appears to be an incomplete recitation of the second Claim 46, and has been disregarded. Applicant is further required to delete the first, incomplete Claim 46.

Claim Rejections - 35 USC § 112

7. The rejection of Claims 1-12, 14, 19-21, 25-40, and 45 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement is withdrawn in light of the amendments to the claims. The rejection of Claim 23 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement is withdrawn in light of the amendments to the claims and Applicant's arguments.The rejection of Claims 3, 7-10, 15-18, 22, 23, 25, 27-35, 37-40, 42-44, and 46-68 under 35 U.S.C. 112, second paragraph, as being indefinite is withdrawn in light of the amendments to the claims. The rejection of Claim 14 under 35 U.S.C. 112, second paragraph, is maintained as per the response to arguments above. The rejection of Claims 1-12, 14, 19-22, 24-40, and 45 under 35 U.S.C. 112, second paragraph, as incomplete is withdrawn.The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claim 14 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically, Claim 14 recites the limitation "without a smart card". Although a negative limitation is not inherently indefinite, the recited limitation renders the claim indefinite because the specification does not provide adequate and enabling written description of what else the separate unit could be apart from a smart card or a SIM card, which is itself a type of smart card. See the response to arguments above, and see also MPEP § 2173.05(i).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1, 3-12, 14-19, 21-24, 27-40, 42-44, and 46-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa, PCT Publication WO97/24831, in view of Anvret et al, European Publication EP 0538216.

In reference to Claim 1, Ichikawa discloses a method that includes connecting a wireless communication apparatus to a separate unit; accessing a wireless communication network (page 2, line 16-page 3, line 12); transmitting a request, which includes information on which of at least one algorithm the wireless apparatus supports, from the wireless apparatus to a data communication apparatus (page 10, line 14-page 11, line 11); the data communication apparatus choosing an algorithm and transmitting a message, which includes information about the chosen algorithm, to the wireless apparatus (page 9, lines 13-23); the wireless apparatus generating a master secret

code (page 4, lines 10-12) and calculating a signature based on the chosen algorithm and the master secret code (page 4, lines 12-15); and saving the master secret code on a memory means of the separate unit and in the data communication apparatus (page 7, line 3-page 8, line 4). However, Ichikawa does not explicitly disclose the use of public and private keys.

Anvret discloses a method that includes the use of public and private keys in message communication (column 6, lines 1-11 and 47-48); transmitting a message, which includes the public key, to a wireless communication apparatus (column 6, lines 39-41); transmitting a response, which includes a calculated signature, to a data communication apparatus (column 6, lines 28-41); the data communication apparatus calculating a master secret code based on a chosen algorithm, a received signature, and the private key; and establishing a secure connection between the wireless apparatus and the data communication apparatus (column 6, line 28-column 7, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Ichikawa's method of generating encryption keys with Anvret's method of identification and exchange of encryption keys, in order to promote the usage of smart cards that enable strong algorithms and enhanced security (see Anvret, column 1, lines 23-25).

In reference to Claim 3, Anvret further discloses re-establishing a connection by transmitting a request, which includes a calculated signature based on the algorithm, public key, and stored secret, from the wireless apparatus to the data communication apparatus (column 6, lines 1-11, 39-41, and 47-48). Anvret additionally discloses that

the data communication apparatus calculates the master secret code based on the algorithm, signature, and private key, and establishes a secure connection to the wireless apparatus (column 6, line 28-column 7, line 13).

In reference to Claim 4 and 27, Ichikawa further discloses that the separate unit is a smart card (page 2, lines 16-25).

Claims 5, 15, 19, 22-24, and 46 each recite limitations recited in, and are substantially equivalent to, Claim 1. The claims are therefore rejected by a similar rationale.

In reference to Claim 6, Anvret further discloses a wireless communication apparatus having an exchangeable memory means (column 2, lines 37-41). Ichikawa further discloses an exchangeable means (namely the smart card of page 2, lines 16-25).

In reference to Claims 7-10, 28-35, 48, 49, and 52-55, Ichikawa further discloses that the master secret code and signature are each stored and generated on the separate unit (Figure 1; page 4, lines 2-15).

In reference to Claims 11, 18, 21, 36-40, 43, 44, and 56-64, Ichikawa further discloses that the separate unit is a smart card (page 2, lines 16-25).

In reference to Claims 12 and 65-68, Ichikawa further discloses that the separate unit is a subscriber identity module (page 2, lines 16-25).

In reference to Claim 14, Ichikawa further discloses an apparatus without a smart card (page 2, lines 16-25).

In reference to Claim 16, Ichikawa further discloses encryption means for encrypting the master secret (page 11, line 19-page 12, line 2).

In reference to Claims 17 and 42, Ichikawa further discloses a secure database including at least one master code or signature (page 4, lines 12-15; Figure 5; page 7, line 9-page 8, line 10; page 11, line 19-page 12, line 2).

Claim 47 corresponds substantially to Claim 3, and is rejected by a similar rationale.

In reference to Claims 50 and 51, Ichikawa further discloses a processor generating the master secret code (page 4, lines 2-15).

13. Claims 2, 20, 25, 26, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa in view of Anvret as applied to claims 1 and 19 above, and further in view of Weiss, US Patent 5845519.

In reference to Claims 2 and 20, Ichikawa as modified discloses everything as applied to Claims 1 and 19 above. However, neither Ichikawa nor Anvret explicitly discloses saving the master secret for a predefined time. Weiss discloses saving a master key for a predetermined time (column 12, lines 40-61). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Ichikawa and Anvret's method of encryption key exchange with Weiss' teaching of saving keys for a predefined time, in order to prevent an unauthorized user from compromising the key (see Weiss, column 12, lines 40-61).

Claim 26 corresponds substantially to Claim 3, and is rejected by a similar rationale.

In reference to Claims 26 and 45, Ichikawa further discloses that the separate unit is a smart card (page 2, lines 16-25).

Conclusion

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER